Upgrading Cisco DCNM for LAN Fabric Deployment

This section includes instructions for upgrading your Cisco DCNM Appliance installation in the following scenarios:

Cisco DCNM Installer version	Release from which you can upgrade
DCNM 11.0(1)	DCNM 10.4(2)

Note When upgrading to a newer DCNM version, you should use the same administrative password (as used in the existing setup) for the new DCNM setup. If you want to use a different password in the new setup, change the password in the existing DCNM setup before taking a backup and initiating the upgrade process.

The following table summarizes the upgrade options for Cisco DCNM 11.0(1).

Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application might not function properly:

- It must be at least 8 characters long and contain at least one alphabet and one numeral.
- It can contain a combination of alphabets, numerals, and special characters.
- Do not use any of these special characters in the DCNM password for all platforms:

  <SPACE> " & $ % ' ^ = < > ; : ` \ | / , .*
- From Cisco DCNM Release 11.0(1), the characters that are allowed in the Administrative password is restricted for OVA and ISO installations. Therefore while upgrading, the old password used in DCNM 10.4(2) is not valid. However, different passwords are allowed during Upgrade.

  The new Administrative password that is entered is used in the following scenarios.

  - accessing the DCNM appliance via its console.
  - accessing the appliance via SSH
  - for applications running on the appliance, e.g. Postgres DBMS

However, after the upgrade, since Postgres DBMS is restored from the backup that is taken on DCNM 10.4(2), you must logon to the Cisco DCNM Web UI using the password used on DCNM Release 10.4(2) appliance.

Clear the browser cache before you launch the Cisco DCNM Web UI using the Management Network IP address, after upgrade. For instructions on how to clear the browser cache, see Clearing Browser Cache.

This chapter contains the following:

Upgrading ISO or OVA using the DCNM Upgrade Tool

This section contains the procedure to download **DCNMUpgradeTool** and upgrade DCNM to the latest version.

Downloading the DCNM Upgrade Tool

The first step to upgrading the DCNM is to download the DCNMUpgradeTool script.

Note If you plan to use HA application functions, you must deploy the `dcnm.ova` or `dcnm.iso` file twice.

Procedure

Step 1 Go to the following site: http://software.cisco.com/download/ .

Step 2 In the Select a Product search box, enter **Cisco Data Center Network Manager**.

Click the **Search** icon.

Step 3 Click on **Data Center Network Manager** from the search results.

A list of the latest release software for Cisco DCNM available for download is displayed.

Step 4 In the Latest Releases list, choose Release 11.0(1).

Step 5 Locate the DCNM Upgrade Tool and click **Download** icon.

Save the file to the appliance `/root` directory.

Backup Using the Upgrade Tool

Beginning with Release 11.0(1), you can download the DCNMUpgradeTool from the Software Downloads page, to take a backup of the DCNM Appliance. This data from this backup file is restored after you upgrade the appliance to DCNM Release 11.0(1).

Perform the following task to run the DCNMUpgradeTool to take a backup of all the applications and data on DCNM 10.4(2).

Before you begin

Ensure that you have copied the DCNMUpgradeTool script to the /root directory of your appliance. Enable read and write permissions on the script using the **chmod 777** or **chmod +x** command.

Procedure

Step 1 Copy the **DCNMUpgradeTool** to the root folder of the Cisco DCNM server.

Step 2 Execute the upgrade tool command.

```
dcnm1# ./DCNMUpgradeTool
```

The tool will analyse the DCNM appliance data and decide if you can upgrade to 11.0(1) or not.

Note The backup that is generated by using this tool can be used to restore data, after upgrade.

Step 3 Enter **y** to continue.

Example:

```
Continue? [y/n] y
```

The tool inspects the systems, checks all constraints, and determines whether the appliance can be upgraded. It also checks for any SAN configuration and default fabrics. If the upgrade criteria is met, the system displays as shown below.

```
This system version: 10.4(2)

- Checking SAN config
- Checking default fabric
...

Congratulations! You can upgrade to DCNM 11.0(1)
```

If the criteria is not met, the upgrade is terminated.

Step 4 Enter **y** to create a backup file.

```
Create backup file? [y/n]: y
```

After the backup is completed successfully, the following message is displayed.

```
**************************************************
Backup is available at /root/backup.DD_MM_YYYY_HH_MM_SS.tar.gz
**************************************************
```

Copy the backup file to a safe location and shut down the application.

Upgrading and Restoring DCNM Virtual Appliance in Standalone mode

Note This procedure applied to both DCNM OVA and ISO upgrade.

Perform the following task to upgrade the DCNM appliance and restore data.

Before you begin

Ensure that you have copied the backup generated from `DCNMUpgradeTool` to a safe location.

Procedure

Step 1 Update the interface MAC address of the Active and Standby appliance. Right-click on **VM > Edit Settings > Hardware**.

For both Network Adapters, update the MAC address to be the same as Cisco DCNM 10.4(2). This ensures that the same MAC address is used for the new Virtual Machine (VM); licenses on Cisco DCNM will not need to be regenerated in the event of an upgrade.

Step 2 Right click on the OVF and select **Power > Power on**.

Step 3 After the VM is powered on click on **Console** tab.

A message indicating that the DCNM appliance is configuring appears on the screen.

Copy and paste the URL to the browser to continue with restore process.

Step 4 On the Cisco DCNM Web Installer UI, click **Get Started**.

Step 5 On the Cisco DCNM Installer screen, select **Fresh Installation with backup file for upgrade or restore** radio button.

Click **Continue**.

Step 6 Select the backup file that was generated using the `DCNMUpgradeTool`.

You can choose perform either on one of the following.

- Click **Upload backup file**. Navigate to the backup file generated for the Active node. Select the appropriate backup file. Click **OK**.
- Click **Copy remote backup file**. Provide the Remote machine information.

  Note You must SSH or RSync must be installed on the Remote machine.

  Click **OK**.

Verify if the correct backup filename appears in the Select backup file field. Click **Continue**.

Note If the backup file was generated without using the **DCNMUpgradeTool**, an error appears and you will not be able to upgrade the DCNM.

Step 7 After the backup file is uploaded, the DCNM server will read and auto-populate the values in some fields.

The prefill is based on the content of the backup file that was provided. You can verify the values and modify if necessary.

Step 8 In the Administration tab, ensure that the correct password is entered.

Click **OK** on the Note pop-up message.

Click **Next**.

Step 9 In the Install Mode tab, from the drop-down list, choose Easy Fabric installation mode for the OVA DCNM Appliance.

Note Only the supported upgrade mode will appear in the drop down list. For more information, see Upgrade Paths.

Click **Next**.

Step 10 On the System Settings, verify the Hostname, DNS Server Address and NTP server information.

Modify the configuration, if required and click **Next**.

Step 11 On the Network Settings tab, verify the network settings configuration.

Modify the configuration if required and click **Next**.

Step 12 On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** complete Cisco DCNM Virtual Appliance Installation for the chosen deployment mode.

A progress bar appears showing the completed percentage, description of the operation, and the elapsed time during the installation.

After the progress bar shows 100%, click **Continue**.

A warning message appears with information to restore the Release 10.4(x) data to the upgraded appliance.

```
Your Cisco Data Center Network Manager software has been installed.
However, data in backup file has not been restored yet.
To complete restore or upgrade, please SSH into the appliance and run the following command:
appmgr restore/root/backup.tar.gz.
```

Step 13 Logon to the Active appliance using SSH. Restore the data on the DCNM appliance using the following command:

appmgr restore /root/backup.tar.gz

The system performs some validations, and the information is displayed.

- Backup version
- Current DCNM version
- Backup System type

Step 14 Click **y** to proceed to restore the backup data.

Example:

```
Do you want to proceed? [y/n] y
```

Step 15 After the data is restored, check the status using the **appmr status all** command.

What to do next

Logon to the DCNM Web UI with appropriate credentials.

Note Logon to the Cisco DCNM Web UI using the password used on DCNM Release 10.4(2) appliance.

Ensure that you clear the browser cache before you launch the Cisco DCNM Web UI using the Management Network IP address.

Click **Settings** icon and choose **About DCNM**. You can view and verify the Installation type that you have deployed.

To gracefully onboard Cisco DCNM 10.4(2) managed VXLAN BGP EVPN fabric(s) comprising Cisco Nexus 9000 switches post upgrade to DCNM 11.0(1), see Post DCNM 10.4(2) to DCNM 11.0(1) Upgrade Procedure for VXLAN BGP EVPN Fabrics.

Upgrading and Restoring DCNM Virtual Appliance in Native HA Mode

The native HA is only supported on DCNM appliances with ISO or OVA installation. Unlike HA mechanisms, it doesn't require any external dependencies like an Oracle database or a shared NFS file system.

The native HA feature allows two Cisco DCNM appliances to run as active and standby applications, with their embedded databases synchronized in real time. Therefore, when the active DCNM is not functioning, the standby DCNM takes over with the same database data and resume the operation.

Perform the following to upgrade the Cisco DCNM Native HA appliances to Release 11.0(1).

Before you begin

Ensure that both the Cisco DCNM 10.4(2) Active and Standby peers are up and running.

Procedure

Step 1 Copy the DCNMUpgradeTool to the root folder of both Active and Standby servers.

Note For example, let us indicate Active and Standby appliances as dcnm1 and dcnm2 respectively.

Step 2 Check and ensure that the Active and Standby servers are operational, by using the **appmgr show ha-role** command:

Example:

On the Active node:

```
dcnm1# appmgr show ha-role
Native HA enabled.
Deployed role: Active
Current role: Active
```

On the standby node:

```
dcnm2# appmgr show ha-role
Native HA enabled.
Deployed role: Standby
Current role: Standby
```

Step 3 Run the DCNMUpgradeTool on both the DCNM 10.4(2) appliances and save the backup to your local directory.

For instructions, see Backup Using the Upgrade Tool, on page 2.

Check if separate `.tar` archives are stored in an external file system.

Step 4 Copy the interface MAC address of the Active and Standby appliance. Right-click on **VM > Edit Settings > Hardware**.

For both Network Adapters, update the MAC address to be the same as Cisco DCNM 10.4(2). This ensures that the same MAC address is used for the new Virtual Machine (VM); licenses on Cisco DCNM will not need to be regenerated for the appliances after upgrade.

Step 5 Shut down both the appliances using the **shutdown -h** command.

You can also right on the VM, select **Power > Power Off**.

Example:

```
dcnm1# shutdown -h now
dcnm2# shutdown -h now
```

Step 6 Install Cisco DCNM 11.0(1) on two appliances, one for Active and one for Standby.

You can either deploy DCNM as OVA or ISO. You must first deploy OVA as an OVF template, or configure KVM or Baremetal for ISO installation. For instructions, see:

- OVA—Deploying the Open Virtual Appliance as an OVF Template
- ISO—either one of the following.
  - Installing the DCNM ISO Virtual Appliance on KVM
  - Installing the DCNM ISO Virtual Appliance on UCS (Bare Metal)

Note If this deployment is a part of the upgrade process, do not Power on the VM. Edit and provide the 10.4(2) MAC address and power on the VM.

Step 7 Update the interface MAC address of the Active and Standby appliance. Right-click on **VM > Edit Settings > Hardware**.

For both Network Adapters, update the MAC address to be the same as Cisco DCNM 10.4(2). This ensures that the same MAC address is used for the new Virtual Machine (VM); licenses on Cisco DCNM will not need to be regenerated in the event of an upgrade.

Step 8 After the VM or Baremetal is powered on, click **Console** tab.

Note Before you power on the VM, ensure that you have reserved appropriate resources for the VM, such as CPU and memory, based on the chosen deployment configuration.

A message indicating that the DCNM appliance is configuring appears on the screen.

Copy and paste the URL to the browser to continue with restore process.

Step 9 On the Active node DCNM Web Installer UI, upload and validate the backup file.

a) Click **Get Started**.

b) On the Cisco DCNM Installer screen, select **Fresh Installation with backup file for upgrade or restore** radio button.

Click **Continue**.

c) Select the Active node backup file that was generated using the `./DCNMUpgradeTool` script.

You can choose perform either on one of the following:

- Click **Upload backup file**.

  Navigate to the backup file generated for the Active node. Select the appropriate backup file. Click **OK**.

- Click **Copy remote backup file**.

  Provide the Remote machine information. Click **OK**.

Verify if the correct backup file name appears in the Select backup file field. Click **Continue**.

Note If the backup file was generated without using the DCNMUpgradeTool, an error appears and you will not be able to upgrade the DCNM.

d) After the backup file is uploaded, the DCNM server will read and auto populate the values in some fields.

The prefill is based on the content of the backup file that was provided.

e) In the Administration tab, ensure that the correct password is entered and click **Next**.

f) In the Install Mode tab, from the drop-down list, choose Easy Fabric installation mode for the OVA DCNM Appliance.

Note Only the supported upgrade mode appears in the drop-down list. Refer to b_dcnm_installation_guide_for_lan_fabric_11_0_1_chapter1.pdf#nameddest=unique_6 unique_6_Connect_42_Upgrade-Paths-to-aragon, for more information.

Click **Next**.

g) On the System Settings, verify the Hostname, DNS Server Address, and NTP server information.

Modify the configuration, if necessary and click **Next**.

h) On the Network Settings tab, verify the network settings configuration.

Modify the configuration if necessary and click **Next**.

i) On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** complete Cisco DCNM Virtual Appliance Installation for the chosen deployment mode.

A progress bar appears showing the completed percentage, description of the operation, and the elapsed time during the installation.

After the progress bar shows 100%, click **Continue**.

A warning message appears with information to restore the Release 10.4(2) data to the upgraded appliance.

```
Your Cisco Data Center Network Manager software has been installed.
However, data in backup file has not been restored yet.
To complete restore or upgrade, please SSH into the appliance and run the following
command:
appmgr restore /root/backup.tar.gz.
```

Step 10 Log on to the Active appliance using SSH. Restore the data on the DCNM appliance using the **appmgr restore** command.

Note Ensure that the Standby appliance is operational before you run the **appmgr restore** command on the DCNM Active appliance.

```
dcnm1 # appmgr restore /root/backup.tar.gz
Checking backup file and system information...

Backup DCNM version: 10.4(2)
This DCNM version: 11.0(1)
Backup System Type: HA-Primary
```

```
Data in backup file /tmp/uploads/backup.primary.tar.gz, taken on DCNM version 10.4(2),
is going to be restored on this newer DCNM, version 10.0(1).

Native HA will be set up on this system. This will
require the standby node to be up and running.

NOTE: this backup was taken on the PRIMARY node of an HA System.
      Such backup MUST have been taken when the primary node was
      in HA ACTIVE state.

      *** IF PRIMARY WAS NODE WAS NOT IN HA ACTIVE STATE WHEN***
      ***BACKUP WA STAKEN, THE SYSTEM CANNOT BE RESTORED CORRECTLY***
      ***AND YOU WILL EXPERIENCE DATA LOSS***

Do you want to proceed? [y/n]:
```

Step 11 Click **y** to proceed with the restoring the Active appliance.

Step 12 At the prompt, after the data is restored, check the status of the appliance using **appmgr status all**.

Step 13 Verify the role of the Active appliance.

```
dcnm1# appmgr show ha-role
Native HA enabled.
Deployed role: Active
Current role: Active
dcnm1#
```

Step 14 On the Standby node, log on to the Web Installer and perform steps in Installing DCNM 11.0(1) on the Standby appliance.

Step 15 Log on to the Standby appliance using SSH. Restore the data on the DCNM appliance using the **appmgr restore** command.

```
dcnm2 # appmgr restore /root/backup.tar.gz
Checking backup file and system information...

Backup DCNM version: 10.4(2)
This DCNM version: 11.0(1)
Backup System Type: HA-Secondary

Data in backup file /tmp/uploads/backup.secondary.tar.gz, taken on DCNM version 10.4(2),
is going to be restored on this newer DCNM, version 10.0(1).

Native HA will be set up on this system.

NOTE 1: this backup was taken on the PRIMARY node of an HA System.
        Such backup MUST have been taken when the primary node was
        in HA ACTIVE state.

        *** IF PRIMARY WAS NODE WAS NOT IN HA ACTIVE STATE WHEN***
        ***BACKUP WA STAKEN, THE SYSTEM CANNOT BE RESTORED CORRECTLY***
        ***AND YOU WILL EXPERIENCE DATA LOSS***

NOTE 2: PRIMARY/ACTIVE NODE MUST HAVE BEEN ALREADY RESTORED
Have you already restored the primary/active node? [y/n]:
```

Note If you click **n** to confirm that the Active appliance is not restored, the system displays an error and terminates restoring the data.

Step 16 Click **y** to confirm that the Active appliance data is restored.

After the data is restored, a success message appears.

Step 17 After the data is restored, check the status using the **appmr status all** command on both Active and standby nodes.

Step 18 Verify the role of the appliances using the **appmgr show ha-role** command.

Step 19 Log on to the DCNM Web UI with appropriate credentials.

Note After the upgrade, since Postgres DBMS is restored from the backup that is taken on DCNM 10.4(2), you must log on to the Cisco DCNM Web UI using the password used on DCNM Release 10.4(2) appliance.

Ensure that you clear the browser cache before you launch the Cisco DCNM Web UI using the Management Network IP address.

Click **Settings** icon and choose About DCNM. You can view and verify the Installation type that you have deployed.

What to do next

To gracefully onboard Cisco DCNM 10.4(2) managed VXLAN BGP EVPN fabric(s) comprising Cisco Nexus 9000 switches post upgrade to DCNM 11.0(1), see Post DCNM 10.4(2) to DCNM 11.0(1) Upgrade Procedure for VXLAN BGP EVPN Fabrics.